KERANGKA KERJA PEMILIHAN KONTROL TI MENGGUNAKAN PENDEKATAN RISIKO DAN EXPECTED MONETARY VALUES

Supriyono
Jurusan Manajemen Informatika, Program Pendidikan Vokasi, Universitas Brawijaya
Jalan Veteran 12 – 16 Malang 65145
Email : priyono.mipa@gmail.com

ABSTRAK

Analisis risiko merupakan bagian terpenting dari kegiatan proses manajemen risiko. Proses tersebut terdiri dari keseluruhan kegiatan menganalisis risiko dan mengevaluasi risiko. Evaluasi risiko merupakan proses yang digunakan untuk menentukan prioritas yang diberikan oleh manajemen risiko dengan cara membandingkan tingkatan suatu risiko dengan standard yang digunakan, target ataupun kriteria lainnya yang telah ditentukan oleh pihak manajemen. Proses evaluasi risiko terdapat keterkaitan dengan beberapa kebutuhan dari berbagai macam pengguna bisnis dan penyedia layanan Teknologi Informasi (TI) seperti ketersediaan layanan, pemeliharaan, kapasitas dan kualitas.

Terdapat beberapa kontrol TI yang dapat digunakan pada perusahaan tetapi semuanya tidak harus digunakan. Dalam penelitian ini diusulkan kerangka kerja pemilihan kontrol TI berdasarkan pendekatan risiko dan menentukan expected monetary values sesuai dengan standard yang digunakan. Pemilihan kontrol TI tidak berkaitan dengan kerangka kerja tertentu.

Uji coba dilakukan dengan menggunakan beberapa kontrol TI dan risiko yang sudah teridentifikasi. Setelah itu menentukan expected monetary values dan pemeringkatan kontrol TI dengan menggunakan metode cumulative voting. Dari hasil uji coba dihasilkan diantaranya semakin tinggi peringkat kontrol TI maka semakin tinggi peluang kontrol TI untuk mengurangi risiko. Biaya kontrol TI mempengaruhi pengurangan risiko yang sudah teridentifikasi. Semakin tinggi biaya kontrol TI maka semakin besar peluang untuk mengurangi risiko.

***Kata Kunci**: expected monetary values*, kontrol TI, risiko, *cumulative voting*.

1 PENDAHULUAN

Teknologi Informasi merupakan perihal yang sangat penting bagi perusahaan atau organisasi. Teknologi Informasi tersebut dapat digunakan dalam pengambilan suatu keputusan. Semakin berkembangnya Teknologi Informasi, semakin terdapat berbagai macam jenis risiko pada saat pengambilan keputusan. Penelitian Boehm [1] menjelaskan bahwa mengidentifikasi risiko adalah awal dari pengembangan sistem perangkat lunak serta dapat membantu mencegah kerusakan sistem. Penelitian Boehm [1] menyebutkan bahwa manajemen risiko terdiri dari penilaian risiko dan kontrol risiko.

Penelitian Haitao [2] mengusulkan model pengambilan keputusan untuk membangun sistem pencegah kejahatan agar dapat mengurangi kerugian yang disebabkan oleh risiko. Penelitian tersebut dari segi pengambil keputusan, mengusulkan model pengambilan keputusan untuk membangun sistem pencegah kejahatan.

Penelitian Liu [5] membangun sebuah kerangka kerja untuk mengintegrasikan ketersediaan penilaian risiko dari sudut pandang yang berbeda. Tujuan penelitian tersebut adalah membentuk kerangka kerja penilaian risiko untuk mengatasi tantangan yang ada dengan mengadopsi kerangka kerja *IT Infrastructure Library* (ITIL).

Pada penelitian ini diusulkan kerangka kerja untuk memilih kontrol TI menggunakan pendekatan risiko dan *expected monetary values* (EMV). Metodologi yang digunakan merupakan pengembangan penelitian sebelumnya yang dilakukan Haitao [2] dan mengadopsi kerangka kerja penilaian risiko yang dibangun pada penelitian Liu [5]. Pengembangan yang dilakukan dengan menambahkan pemeringkatan kontrol TI menggunakan *cumulative voting* atau metode 100 poin. Kontrol TI berdasarkan standard yang ada diantaranya menggunakan ISO 17799, ITIL, COBIT atau menggunakan standard lainnya. Pemilihan kontrol TI pada penelitian ini tidak berkaitan dengan kerangka kerja tertentu. Pemilihan kontrol TI bertujuan untuk mengatur manajemen risiko dengan cara mengurangi risiko yang ada dengan memilih kontrol TI yang sesuai. Metode yang digunakan pada penelitian ini menggunakan metode 100 poin untuk menentukan pemeringkatan kontrol TI.

2 MODEL, ANALISIS, DESAIN, DAN IMPLEMENTASI

Kerangka kerja yang dibangun bertujuan untuk melakukan pemilihan kontrol TI. Berikut ini dibahas yang berkaitan dengan kerangka kerja yang dibangun.

2.1 Manajemen Risiko

Risiko didefinisikan sebagai peluang terjadinya sesuatu yang dapat memberikan dampak atau mengakibatkan terganggunya proses bisnis organisasi sehingga dapat menyebabkan gagalnya tujuan bisnis organisasi. Risiko kesalahan dapat dikelompokkan menjadi risiko yang melekat, risiko pengendalian dan resiko pendeteksian [10].

a. Risiko yang melekat

Risiko kesalahan tersebut bersifat independen dan semakin tinggi jika kompensasi kontrol tidak tersedia. Contoh risiko kesalahan jenis ini adalah proses bisnis yang melibatkan perhitungan kompleks yang cenderung lebih dekat dengan kesalahan penghitungan yang menyebabkan tingkat risiko semakin tinggi. Contoh lain adalah tanggung jawab terhadap eksekusi proses yang dipegang oleh satu orang padahal seharusnya oleh beberapa orang.

b. Risiko pengendalian

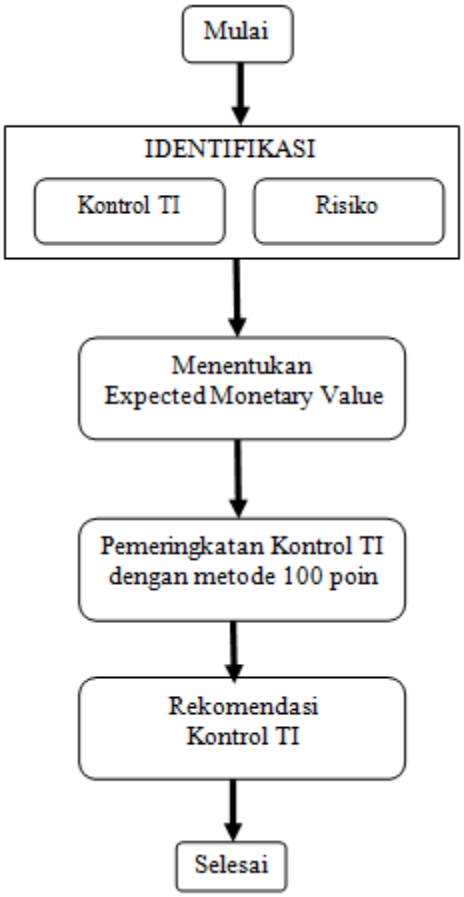
Risiko pengendalian merupakan risiko kesalahan yang tidak terdeteksi oleh kontrol internal itu sendiri selama proses berlangsung. Contoh risiko pengendalian adalah kesalahan pencocokan hasil manual dari catatan komputer dengan tinjauan manual dapat dikategorikan dalam risiko yang tinggi karena aktivitas peninjauan manual membutuhkan penyelidikan yang terkadang sering salah dan kurang tepat. Risiko kontrol tersebut menjadi rendah jika prosedur validasi tersebut dilakukan secara terkomputerisasi.

c. Risiko pendeteksian

Risiko pendeteksian kesalahan dapat dilakukan setelah kesalahan dari proses bisnis terjadi.

2.2 Desain Kerangka Kerja Pemilihan Kontrol TI

Pada bagian ini mengidentifikasi kebutuhan yang berkaitan dengan pengujian model dan teori yang dapat dibuktikan kebenarannya secara ilmiah. Identifikasi kebutuhan penelitian yang dilakukan bertujuan agar penelitian dapat lebih fokus dalam penyelesaian permasalahan. Hasil identifikasi kebutuhan yang diperoleh terdiri dari kontrol TI, daftar risiko beserta biaya yang dikeluarkan. Identifikasi yang berkaitan dengan kontrol TI dapat menggunakan COBIT, ITIL atau ISO 17799. Untuk mencapai tujuan penelitian maka disusun langkah-langkah rinci seperti pada gambar 1 yang menunjukkan tahapan dalam pemilihan kontrol TI.



Gambar 1. Kerangka Kerja Pemilihan Kontrol TI

2.3 Identifikasi Kontrol TI dan Risiko

Identifikasi kontrol TI dan risiko dilakukan oleh orang yang ahli dibidang kontrol TI. Identifikasi kontrol TI dan risiko terdapat dua hal yaitu identifikasi yang bersifat ekstrim dan non ekstrim. Identifikasi kontrol TI dan risiko yang ekstrim dapat berdasarkan ISO/IEC 27001 maupun standard COBIT dan ITIL.

2.4 Menentukan EMV

Penelitian berikut ini menggunakan pendekatan EMV karena dapat digunakan untuk mengurangi risiko dengan melakukan pemilihan kontrol TI yang sesuai berdasarkan standard kontrol TI. Selain itu biaya yang dikeluarkan tidak melebihi dari investasi suatu perusahaan atau organisasi. Langkah-langkah penentuan EMV.

1 Inisialisasi *Original Risk Loss* Matriks E

Original Risk Loss pada Matriks E menggambarkan kerugian dari sisi ekonomi. Dimana e_i merepresentasikan kerugian ekonomi yang disebabkan oleh risiko dan nilai i=1,2,3,...,n.

$$\begin{bmatrix} e_1 & 0 & \cdots & 0 \\ 0 & e_2 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & e_n \end{bmatrix}$$

2 Inisialisasi *Feasible Strategy* Matriks *S*

s_i merepresentasikan biaya dari sistem pencegah kejahatan yang disebut dengan *Feasible Strategies Set*. Dimana nilai *i*= 1,2,3,..n.

$$\begin{bmatrix} s_1 \\ s_2 \\ \vdots \\ s_m \end{bmatrix}$$

Menginisialisasi Strategi yang mungkin pada Matriks S.

3 Membangun kinerja sistem Matriks P

Pada umumnya tugas seorang ahli risiko dan ahli sistem informasi adalah mengevaluasi hasil dari sistem yang dibangun dan mengukur hasil dari sistem pencegah kejahatan p_{ij} (i=1,2,...,n; j=1,2,..,m), $p_{ij} \epsilon$ [0,1], yang mana menunjukkan kerugian ekonomi yang disebabkan risiko r_j akan direduksi e_j x p_{ij} jika sebuah sistem pencegah kejahatan dari biaya s_j yang dibangun. Indeks *i* menunjukkan baris dan indeks *j* menunjukkan kolom pada matriks P. Kinerja sistem matriks P adalah sebagai berikut ini.

$$\begin{bmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ p_{1m} & p_{2m} & \cdots & p_{mn} \end{bmatrix}$$

Rentang nilai kinerja sistem matriks P antara 0 sampai dengan 1. Nilai yang mendekati 1 menunjukkan kemampuan dalam mengurangi risiko mempunyai peluang yang lebih besar. Sedangkan nilai yang mendekati 0 menunjukkan peluang mengurangi risiko lebih kecil. Dari hasil evaluasi untuk membangun sistem maka dapat dihasilkan suatu matriks P.

4 Membangun Probabilitas Risiko Matrix L

Dalam membangun kemungkinan risiko digunakan teknik analisis statistik yang dapat ditentukan dengan frekuensi $F(f_1,f_2,...,f_n)$. Probabilitas matriks L dibentuk dengan cara analisis histori data risiko yang sudah diidentifikasi. l_i menunjukkan kemungkinan dari risiko r_i dimana i = 1,2,3,...,n.

$$\begin{bmatrix} l_1 & 0 & \cdots & 0 \\ 0 & l_2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & l_n \end{bmatrix}$$

Relasi antara l_i (i=1,2,3...,n) dan f_i (i=1,2,3...,n) menggunakan persamaan sebagai berikut ini.

$$li = \frac{fi}{\sum_{i=l}^{n} fi} \qquad (1)$$

dimana l_i adalah probabilitas risiko ke *i* dan f_i adalah frekuensi ke *i*. Nilai *i* = 1,2,3,...n.

5 Membangun risiko EMV Matrix Q

Hasil EMV ditunjukkan dengan notasi $a_{11},a_{12},...a_{mn}$. Berikut ini matriks Q yang dihasilkan.

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Persamaan yang digunakan untuk menghitung EMV adalah sebagai berikut ini.

$$Q=P \text{ x } E \text{ x } L \qquad (2)$$

dimana Q adalah EMV, P adalah kinerja sistem matriks, E adalah *Original Risk Loss* Matriks E, dan L adalah probabilitas risiko matriks L.

2.5 Pemeringkatan Kontrol TI dengan Metode 100 Poin

Pada tahapan proses ini menggunakan metode 100 poin. Langkah-langkah dalam pemeringkatan kontrol TI dengan menggunakan metode 100 poin adalah sebagai berikut ini.

a. Memasukan semua kontrol TI yang digunakan dalam satu baris.
b. Membagi semua poin diantara kontrol TI yang digunakan menurut yang paling sesuai dengan sistem kontrol yang ada dari setiap orang yang berkontribusi.
c. Menjumlahkan poin yang didapat pada setiap kontrol TI dari setiap pemberi poin.
d. Melakukan perangkingan terhadap kontrol TI berdasarkan total poin yang diperoleh.

3 SKENARIO UJI COBA

Pada skenario identifikasi kontrol TI dan identifikasi risiko terdapat dua kategori skenario yang dilakukan yaitu seperti berikut ini.

a. Skenario 1 dengan mengidentifikasi kontrol TI dan risiko yang bersifat ekstrim. Pada skenario 1 terdiri dari identifikasi kontrol TI dan risiko yang memiliki perbedaan yang besar. Skenario 1 ditambahkan kondisi skenario yang biaya kontrolnya lebih kecil daripada biaya pada masing-masing risiko dalam satuan juta rupiah. Skenario berikutnya ditambahkan biaya kontrol lebih besar daripada biaya pada masing-masing risiko dalam satuan juta rupiah. Identifikasi kontrol TI dan risiko pada skenario 1 adalah seperti berikut ini.

Tabel 1. Identifikasi Kontrol TI

K_1	Kontrol jaringan
K_2	Transaksi online
K_3	Penggunaan password
K_4	Batas waktu sesi
K_5	Integritas pesan

Tabel 2. Identifikasi Risiko

R_1	Kebakaran
R_2	Banjir
R_3	Halilintar
R_4	Gempa Bumi
R_5	Gunung meletus
R_6	Angin Topan

b. Skenario 2 dengan mengidentifikasi kontrol TI dan risiko yang bersifat non ekstrim. Pada skenario berikut ini dilakukan identifikasi kontrol TI dan risiko yang bersifat non ekstrim yang terdiri dari identifikasi kontrol TI dan risiko yang memiliki perbedaan yang kecil. Identifikasi dilakukan oleh pihak manajemen atau seseorang yang sudah ahli dibidangnya. Identifikasi kontrol TI dan risiko pada skenario 2 adalah seperti berikut ini.

Tabel 3. Identifikasi Kontrol TI

K_1	Manajemen password pengguna
K_2	Pemeriksaan dari hak akses pengguna
K_3	Kontrol koneksi jaringan
K_4	Sistem manajemen password
K_5	Validasi keluaran data
K_6	Kontrol pada operasi perangkat lunak

Tabel 4. Identifikasi Risiko

R_1	Kesalahan pengguna
R_2	Kesalahan administrator
R_3	Kesalahan konfigurasi
R_4	Gangguan perangkat lunak
R_5	Gangguan program jahat
R_6	Kesalahan informasi yang tidak tepat

4 HASIL UJI COBA

Langkah-langkah penyelesaian pada skenario 1 adalah sebagai berikut ini.

a. Menginisialisasi strategi yang mungkin pada Matriks S. Nilai pada matriks S didapat dari biaya kontrol TI yang sudah diidentifikasi dan ditentukan oleh seorang ahli kontrol TI. Pada skenario 1 dilakukan inisialisasi Matriks S seperti berikut ini.

$$\begin{bmatrix}1\\2\\3\\4\\5\\6\end{bmatrix}$$

b. Menginisialisasi *original risk loss* Matriks E. Nilai pada matriks E didapat dari biaya risiko yang sudah diidentifikasi. Hal tersebut ditentukan oleh seorang ahli kontrol TI. Risiko beserta kerugiannya dibuat sebuah matriks seperti berikut ini.

$$\begin{bmatrix}2&0&0&0&0&0\\0&4&0&0&0&0\\0&0&6&0&0&0\\0&0&0&8&0&0\\0&0&0&0&10&0\\0&0&0&0&0&12\end{bmatrix}$$

c. Membangun kinerja sistem matriks P. Rentang nilai yang dimasukkan oleh seoarang yang ahli dibidang pemilihan kontrol TI antara 0 – 1. Apabila nilai yang dimasukkan mendekati angka 1 maka kontrol TI mempunyai kemungkinan mengurangi risiko yang teridentifikasi. Sebaliknya apabila nilai yang dimasukkan oleh seorang ahli mendekati 0 maka kontrol TI mempunyai kemungkinan tidak dapat mengurangi risiko. Pada matriks P terdiri dari baris dan kolom. Baris menunjukkan kontrol TI yang teridentifikasi sedangkan kolom menunjukkan risiko yang teridentifikasi. Dari hasil evaluasi tersebut untuk membangun sistem dihasilkan matriks seperti berikut ini.

$$\begin{bmatrix}0.5&0.4&0.4&0.5&0.6&0.7\\0.4&0.3&0.3&0.3&0.2&0.5\\0.3&0.2&0.2&0.3&0.4&0.9\\0.2&0.1&0.3&0.3&0.3&0.4\\0.7&0.5&0.8&0.2&0.5&0.7\\0.6&0.4&0.9&0.1&0.5&0.6\end{bmatrix}$$

d. Membangun Probabilitas risiko Matriks L.
Dari hasil analisis risiko didapatkan frekuensi risiko $F = \{7,5,3,8,7,7\}$. Pada persamaan 1 dapat membangun probabilitas risiko matriks L seperti berikut ini.

$$\begin{bmatrix}7/37&0&0&0&0&0\\0&5/37&0&0&0&0\\0&0&3/37&0&0&0\\0&0&0&8/37&0&0\\0&0&0&0&7/37&0\\0&0&0&0&0&7/37\end{bmatrix}$$

e. Menghitung EMV Matriks *Q*. Untuk membangun matriks Q dengan menggunakan persamaan 2 maka didapat Matriks Q sebagai berikut ini.

$$\begin{bmatrix}0{,}1892&0{,}2162&0{,}1946&0{,}8649&1{,}1351&1{,}5892\\0{,}1514&0{,}1622&0{,}1459&0{,}5189&0{,}3784&1{,}1351\\0{,}1135&0{,}1081&0{,}0973&0{,}5189&0{,}7568&2{,}0432\\0{,}0757&0{,}0541&0{,}1459&0{,}5189&0{,}5676&0{,}9081\\0{,}2649&0{,}2649&0{,}3892&0{,}3459&0{,}9459&1{,}5892\\0{,}2649&0{,}2162&0{,}4378&0{,}1730&0{,}9459&1{,}3622\end{bmatrix}$$

Hasil EMV diatas yang menunjukkan nilai tertinggi adalah $2.0432(K_6,R_3)$ yang terdapat pada kode kontrol K_6 dan kode risiko R_3. Kemudian hasil EMV $1.5892(K_6,R_1)$, $1.3622(K_6,R_6)$, $1.1351(K_5,R_1)$, $0.9459(K_5,R_5)$, $0.8649(K_4,R_1)$ dan $0.4378(K_3,R_6)$. Nilai EMV tertinggi menunjukkan peluang kontrol TI mengurangi risiko lebih besar. Peluang kontrol TI yang dapat mengurangi risiko adalah kontrol routing jaringan, integritas pesan, batas waktu sesi dan penggunaan password.

EMV yang didapat pada proses perhitungan tersebut bertujuan untuk mengurangi risiko yang ada sehingga biaya yang dikeluarkan pada risiko tersebut lebih rendah dan biaya pada setiap kontrol TI yang dipilih tidak melebihi biaya investasi sistem yang dibangun. Hasil uji coba pada pemilihan kontrol TI adalah pendekatan EMV dengan parameter biaya kontrol yang lebih besar dari biaya pada masing-masing risiko dalam satuan juta seperti ditampilkan pada Tabel 5.

Tabel 5. Hasil Uji Coba Biaya Kontrol Lebih Besar daripada Biaya Risiko

Kontrol TI	Risiko / Biaya Risiko / Biaya Kontrol	R_1	R_2	R_3	R_4	R_5	R_6
		2	3	4	5	6	7
K_1	3	0,1892	0,1514	0,1135	0,0757	0,2649	0,2649
K_2	5	0,1622	0,1216	0,0811	0,0405	0,2027	0,1622
K_3	7	0,1297	0,0973	0,0649	0,0973	0,2595	0,2919
K_4	9	0,5405	0,3243	0,3243	0,3243	0,2162	0,1081
K_5	11	0,6811	0,2270	0,4541	0,3405	0,5676	0,5676
K_6	13	0,9270	0,6622	1,1919	0,5297	0,9270	0,7946

Pada uji coba skenario 2 dilakukan identifikasi kontrol TI dan risiko yang bersifat non ekstrim. Parameter biaya kontrol lebih kecil dari biaya pada masing-masing risiko dalam satuan juta rupiah. Untuk parameter biaya kontrol lebih besar dari biaya pada masing-masing risiko dalam juta seperti ditampilkan pada Tabel 6.

Tabel 6. Hasil Uji Coba Biaya Kontrol Lebih Kecil daripada Biaya Risiko

Kontrol TI	Risiko / Biaya Risiko / Biaya Kontrol	R_1	R_2	R_3	R_4	R_5	R_6
		6	8	12	14	16	18
K_1	3	0,5676	0,4541	0,3405	0,2270	0,7946	0,7946
K_2	4	0,4324	0,3243	0,2162	0,1081	0,5405	0,4324
K_3	6	0,3892	0,2919	0,1946	0,2919	0,7784	0,8757
K_4	7	1,5135	0,9081	0,9081	0,9081	0,6054	0,3027
K_5	8	1,8162	0,6054	1,2108	0,9081	1,5135	1,5135
K_6	9	2,3838	1,7027	3,0649	1,3622	2,3838	2,0432

Dari hasil uji coba diperoleh nilai EMV tertinggi pada tabel 6 adalah 3,0649 (K_6,R_3), 2,3838 (K_6,R_1), 2,0432 (K_6,R_6), 1,8162 (K_5,R_1). Berdasarkan uji coba didapatkan validasi keluaran data dan kontrol pada operasi perangkat lunak mempunyai peluang lebih besar dalam mengurangi risiko.

Tabel 7. Hasil Uji Coba Biaya Kontrol Lebih Besar daripada Biaya Risiko

Kontrol TI	Risiko / Biaya Risiko / Biaya Kontrol	R_1	R_2	R_3	R_4	R_5	R_6
		3	4	6	7	8	9
K_1	6	0,2838	0,2270	0,1703	0,1135	0,3973	0,3973
K_2	8	0,2162	0,1622	0,1081	0,0541	0,2703	0,2162
K_3	12	0,1946	0,1459	0,0973	0,1459	0,3892	0,4378
K_4	14	0,7568	0,4541	0,4541	0,4541	0,3027	0,1514
K_5	16	0,9081	0,3027	0,6054	0,4541	0,7568	0,7568
K_6	18	1,1919	0,8514	1,5324	0,6811	1,1919	1,0216

Dari hasil uji coba diperoleh nilai EMV tertinggi pada tabel 7 adalah 1,5324 (K_6,R_3), 1,1919 (K_6,R_1), 1,0216 (K_6,R_6), 0,9081 (K_5,R_1). Berdasarkan uji coba didapatkan validasi keluaran data dan kontrol pada operasi perangkat lunak mempunyai peluang lebih besar dalam mengurangi risiko.

Pada uji coba skenario 2 dilakukan pengujian dimana biaya dari risiko adalah bernilai 1 (dalam satuan juta rupiah) sehingga diperoleh matriks E sebagai berikut ini.

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Dari hasil evaluasi diset angka 1 untuk setiap frekuensi risiko sehingga $F = \{1,1,1,1,1,1\}$ yang digunakan untuk membangun probabilitas risiko matriks L seperti berikut ini.

$$\begin{bmatrix} 1/6 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1/6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1/6 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1/6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1/6 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1/6 \end{bmatrix}$$

Tabel 8 Hasil Uji Coba Biaya Risiko diset 1

Kontrol TI	Risiko / Biaya Risiko / Biaya Kontrol	R_1	R_2	R_3	R_4	R_5	R_6
		1	1	1	1	1	1
K_1	6	0,0833	0,0667	0,0500	0,0333	0,1167	0,1167
K_2	8	0,0667	0,0500	0,0333	0,0167	0,0833	0,0667
K_3	12	0,0667	0,0500	0,0333	0,0500	0,1333	0,1500
K_4	14	0,0833	0,0500	0,0500	0,0500	0,0333	0,0167
K_5	16	0,1000	0,0333	0,0667	0,0500	0,0833	0,0833
K_6	18	0,1167	0,0833	0,1500	0,0667	0,1167	0,1000

Hasil penghitungan EMV diperoleh dari yang tertinggi adalah 0,1500 terdapat pada (K_6,R_3), (K_3,R_6). 0,1333 terdapat pada (K_3,R_5). 0,1167 terdapat pada (K_6,R_1), (K_6,R_5), (K_1,R_5), (K_1,R_6).

f. Uji Coba Pemeringkatan Kontrol TI

Hasil yang diperoleh dari penghitungan EMV diperingkatkan dengan metode 100 poin dengan tujuan hasil kontrol TI yang diperoleh sesuai dengan harapan pengguna. Pelanggan mendistribusikan 100 poin ke 10 kontrol TI berdasarkan hasil penghitungan EMV pada skenario 1 seperti pada tabel 9.

Tabel 9. Distribusi Poin oleh Pengguna

Kontrol TI	Poin
K_3	42
K_4	16
K_5	24
K_6	18
Jumlah	100

Tabel 9 menampilkan hasil distribusi poin oleh pengguna melalui pertimbangan dan perbandingan sehingga mendapatkan total semua poin sebesar 100. Kemudian tabel distribusi diurutkan berdasarkan kolom poin. Peringkat 1 diberikan pada kontrol TI dengan prioritas tertinggi. Daftar pengurutan distribusi poin ditunjukkan pada Tabel 10.

Tabel 10. Pengurutan Poin

Kontrol TI	Poin	Peringkat
K_3	42	1
K_5	24	2
K_6	18	3
K_4	16	4

Skenario 1 menunjukkan hasil yang relatif stabil untuk penghitungan EMV. Skenario 2 menunjukkan hasil yang relatif tidak stabil untuk data uji biaya dari risiko dan frekuensi risiko bernilai sama. Data uji coba untuk nilai yang sama diset dengan biaya 1 juta sehingga hasil EMV terdapat banyak kesamaan.

Dari hasil yang diperoleh dapat terlihat bahwa kontrol TI, risiko yang diidentifikasi dan biaya yang dikeluarkan berpengaruh pada pemilihan kontrol TI. Hal itu telah dibuktikan pada skenario uji coba 1 dan skenario uji coba 2. Pada pengujian tersebut terlihat semakin tinggi biaya kontrol TI maka mempunyai hasil EMV yang tinggi. Hasil EMV yang tertinggi mempunyai peluang untuk mengurangi risiko yang cukup besar. Sedangkan hasil EMV yang terkecil mempunyai peluang mengurangi risiko yang kecil.

5 KESIMPULAN

Dari uji coba yang telah dilakukan maka dapat ditarik kesimpulan berikut ini.

1. Pemilihan kontrol TI dengan menentukan EMV dapat dihasilkan lebih dari satu kontrol TI sehingga memudahkan pihak manajemen dalam menentukan kontrol TI yang sesuai dengan kebutuhan. Biaya kontrol TI dan risiko yang ditentukan pihak manajemen kontrol TI dapat mempengaruhi pemilihan kontrol TI. Semakin besar biaya kontrol TI maka semakin berpeluang untuk mengurangi risiko.
2. Metode 100 poin dapat digunakan untuk menentukan peringkat kontrol TI sehingga dapat menentukan prioritas utama kontrol TI. Semakin tinggi peringkat kontrol TI maka semakin tinggi peluang kontrol TI mengurangi risiko.

Untuk meningkatkan hasil yang telah dicapai dari penelitian ini dapat dilakukan beberapa perbaikan sebagai berikut ini.

1. Menambahkan data histori dari setiap pemilihan kontrol TI dan penentuan EMV.
2. Melakukan perbaikan proses pemeringkatan kontrol TI dan penghitungan dari EMV.

6 DAFTAR PUSTAKA

[1] Boehm, Barry W. 1991. "Software Risk Management:Principles and Practices, Defense Advanced Research Projects Agency". IEEE Software, hal 32 – 40.

[2] Haitao Lv. 2011. "Investment Decision Model of Crime Prevention System Based on EMV of the Economic Loss Caused by risks". Third IEEE International Conference on Space Mission Challenges for Information Technology, hal 388 – 392.

[3] Leffingwell, D. dan Widrig, D. 1999. Managing Software Requirements: A Unified Approach, 5rd edition. USA : Addison-Wesley.

[4] Leffingwell, D. dan Widrig, D. 2003. Managing Software Requirements: A Use Case Approach, 2nd edition. pp 124-125. USA : Addison-Wesley.

[5] Liu, Hui, Yue Lin, Peng Chen, Lufeng Jin, Fan Ding. 2010. "A Practical Availability Risk Assessment Framework in ITIL". Fifth IEEE International Symposium on Service Oriented System Engineering, hal 286-290.

[6] Luís Enrique Sánchez, Daniel Villafranca, Eduardo Fernández-Medina, Mario Piattini. 2006. "Practical Approach of a Secure Management System based on ISO/IEC 17799", Proceedings of the First International Conference on Availability, Reliability and Security. ARES '06.

[7] Mayer, Nicolas. 2004. Managing Security IT Risk: a Goal-Based Requirements Engineering

Approach, Luxembourg, Kirchberg : Public Research Centre Henri Tudor 29, av. J. F.Kennedy, L-1855.

[8] Roger S Debreceny. 2006. "Re-engineering IT Internal Controls: Applying Capability Maturity Models to the Evaluation of IT Controls", Proceedings of the 39th Hawaii International Conference on System Sciences. Vol. 8, pp. 196c.

[9] Rabbi, Md. Forhad, Khan Olid Bin Mannan. 2008. "A Review of Software Risk Management for Selection of best Tools and Techniques", Ninth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, hal 773 – 778.

[10] Sarno, Ryanarto. 2009. Audit Sistem dan Teknologi Informasi. Surabaya : ITS Press.

[11] Shoichi Morimoto. 2009. "Application of COBIT to Security Management in Information Systems Development", International Conference on Frontier of Computer Science and Technology.